REMARKS

This Application has been carefully reviewed in light of the Final Office Action mailed July 17, 2006. In order to advance prosecution of this case, Applicants amend Claims 1, 10, 11, 12, and 14. Applicants cancel Claims 5 and 17 without prejudice or disclaimer. Applicants previously canceled Claims 2-3, 6-7, and 18-19 without prejudice or disclaimer. Applicants respectfully request reconsideration and favorable action in this case.

Section 102 Rejections

The Examiner rejects Claims 1, 4-5, and 10-17 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,398,196 issued to Chambers ("*Chambers*"). As amended, Claim 1 includes elements similar to those previously included in Claim 5. Therefore, the rejections of Claim 5 are addressed with respect to amended Claim 1. Claim 1 recites:

> A method of detecting viral code in subject files, comprising:
> creating an artificial memory region spanning one or more components of the operation system;
> creating a custom version of an export table, wherein the custom version of the export table is associated with a plurality of entry points and wherein the entry points comprise predetermined values;
> emulating execution of at least a portion of computer executable code in a subject file;
> monitoring accesses by the emulated computer executable code to the artificial memory region to detect looping in the execution of the emulated computer executable code; and
> determining based on a detection of looping whether the emulated computer executable code is viral.

Chambers fails to recite, expressly or inherently, every element of amended Claim 1. As Applicants previously noted, with respect to previously presented Claim 5, *Chambers* fails to disclose "monitoring accesses by the emulated computer executable code to the artificial memory region to detect looping in the execution of the emulated computer executable code" and "determining based on a detection of looping whether the emulated computer executable code is viral." Applicants respectfully note that the Examiner has not identified any form of "looping." Instead, the Examiner cites to a portion of *Chambers* that discusses repeating the emulation on a second file independent of the first emulation. As Chambers emphasizes "[t]he process of FIG. 10 essentially creates *a completely new emulation*." Col. 10, ll. 37-38. The system of *Chambers* repeats the emulation process unconditionally and, thus, the system

of *Chambers* determines nothing *based on* a detection of looping. Instead, *Chambers* repeats the emulation process and determines based on whether the results of the repeated emulation are the same as the original emulation. As *Chambers* emphasizes:

> *If* this first guinea pig file now passes modification behavior on to a second guinea pig file, *then* the original target program has been shown to be contaminated with viral code having replicative behavior.
>
> Col. 10, ll. 40-44, emphasis and underlining added.

Thus, the emulation process is repeated in all instances, and the system determines *based on the results* of the repeated process whether the relevant code is viral. Not only is this repetitive execution not "looping," as the system completes the emulation process and then restarts it with respect to a second file, but the system does not determine whether the code is viral based on this repetition as the emulation is always repeated. As a result, *Chambers* fails to recite, expressly or inherently, "monitoring accesses by the emulated computer executable code to the artificial memory region *to detect looping in the execution of the emulated computer executable code*" and "determining *based on a detection of looping* whether the emulated computer executable code is viral" as recited by Claim 1. Despite the Examiner's assertions, the Examiner has not rebutted this argument, in the Office Action issued October 31, 2005 or any other Office Actions.

Consequently, *Chambers* fails to disclose every element of amended Claim 1. Claim 1 is thus allowable for at least these reasons. Applicants respectfully request reconsideration and allowance of Claim 1 and its dependents.

Although of differing scope from Claim 1, Claims 10-12 and 14 include elements that, for reasons substantially similar to those discussed with respect to Claim 1, are not disclosed by *Chambers*. Claims 10-12 and 14 are thus allowable for at least these reasons. Applicants respectfully request reconsideration and allowance of Claims 10-12 and 14, and their respective dependents.

Additionally, for the purpose of advancing prosecution, Applicants cancel Claims 5 and 17 without prejudice or disclaimer, thereby obviating the Examiner's rejection of these claims. Applicants wish to note that, with respect to all amendments and cancellations herein, Applicants reserve the right to pursue broader subject matter than that currently claimed through the filing of continuations and/or other related applications.

Section 103 Rejections

The Examiner rejects Claims 8, 9, and 20 under 35 U.S.C. § 103(a) as being unpatentable over *Chambers* in view of U.S. Patent No. 5,974,549 issued to Golan ("*Golan*"). Claims 8 and 9 depend from Claim 1, while Claim 20 depends from Claim 14. Claims 1 and 14 have been shown above to be allowable. Claims 8, 9, and 20 are thus allowable for at least these reasons.

Additionally, Claims 8, 9, and 20 include additional elements not disclosed, taught, or suggested by the cited references. For example, Claim 8 recites:

> The method of claim 1, further comprising monitoring access by the emulated computer executable code to dynamically linked functions.

Chambers and *Golan*, both alone and in combination, fail to disclose additional elements of Claim 8. For example, the proposed *Chambers-Golan* combination fails to disclose "monitoring access by the emulated computer executable code to dynamically linked functions." As the Examiner concedes, "Chambers fails to disclose anything concerning dynamically linked functions." *Office Action*, p. 4.

Moreover, combining *Chambers* with *Golan* fails to remedy this omission as *Golan* also fails to disclose this element. The references to dynamic link libraries (DLLs) in the cited portion of *Golan* indicate only that a DLL can be used *to monitor access to a set of API calls*. *Golan* does not indicate that "access to dynamically linked functions is regulated" as the Examiner suggests. Instead, the DLL itself regulates access *to other components* of the system. Consequently, *Golan* fails to disclose "monitoring access by the emulated computer executable code to dynamically linked functions" and, thus, the proposed *Chambers-Golan* combination also fails to disclose this element.

As a result, the proposed *Golan-Chambers* combination fails to disclose, teach, or suggest additional elements of Claim 8. Although of differing scope from Claim 8, Claims 9 and 20 include additional elements that are not disclosed, taught, or suggested by the proposed *Chambers-Golan* combination. Claims 8, 9, and 20 are thus allowable for at least these additional reasons. Applicants respectfully request reconsideration and allowance of Claims 8, 9, and 20.

Conclusions

Applicants have made an earnest attempt to place this case in condition for allowance. For the foregoing reasons, and for other reasons clearly apparent, Applicants respectfully request full allowance of all pending Claims. If the Examiner feels that a telephone conference or an interview would advance prosecution of this Application in any manner, the undersigned attorney for Applicants stands ready to conduct such a conference at the convenience of the Examiner.

No fees are believed to be due, however, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 02-0384 of Baker Botts L.L.P.

Respectfully submitted,

BAKER BOTTS L.L.P.
Attorneys for Applicants

Todd A. Cason
Reg. No. 54,020

2001 Ross Avenue, Suite 600
Dallas, Texas 75201-2980
(214) 953-6452

Date: 10/17/06

CORRESPONDENCE ADDRESS:

Customer Number: **05073**